Pięć najlepszych sposobów na zwiększenie bezpieczeństwa dzięki sieci

Do zrujnowania firmy wystarczy jedno włamanie do sieci. Zabezpieczenia znajdujące się na jej obrzeżach przestały już wystarczać. Sieć traktowana jako towar nie zapewni niezbędnego poziomu bezpieczeństwa. Potrzebujesz sieci, w której zabezpieczenia są wbudowane – bez ograniczania sprawności działania i tłumienia innowacyjności.

Oto pięć sposobów na zwiększenie bezpieczeństwa sieci.

1

Właściwa osoba, właściwe miejsce, właściwy czas

Niech Twoja sieć na bieżąco powstrzymuje niepożądane działania na swoim terenie. Uprość realizację dostępu do sieci, aby przyspieszyć działanie zabezpieczeń i konsekwentnie egzekwować zasady w każdym miejscu sieci. Klasyfikuj ruch sieciowy na podstawie tożsamości punktów końcowych, nie ich adresów IP. Dzięki temu uniemożliwisz szkodliwym systemom dostęp do sieci i łatwiej zrealizujesz cele związane ze zgodnością.

TrustSec

2

Czy tak powinno być?

Wyjdź poza standardowe wykrywanie zagrożeń i wykorzystaj moc analityki sieci. Stale monitoruj wewnętrzną część sieci – tam często czają się niewykryte, zaawansowane zagrożenia. Zintegruj z siecią funkcje wykrywania anomalii związanych z bezpieczeństwem, wykorzystując uczenie się maszynowe do reagowania na incydenty i eliminowania ich skutków na poziomie urządzeń. Dzięki temu możesz wykryć i zatrzymać ataki przenikające granice sieci i dotykające środowiska wewnętrznego, a także poddawać kwarantannie podejrzane urządzenia.

Stealthwatch

„System Stealthwatch zdobył nagrodę CODiE 2016 dla najlepszego rozwiązania w zakresie bezpieczeństwa sieci”.

3

Kontroluj dostęp

Uprość kontrolę dostępu za pośrednictwem połączeń przewodowych, bezprzewodowych i VPN, kaskadowo stosując do wszystkich typów punktów dostępu te same, definiowane programowo, zasady bezpieczeństwa. Ułatwia to zachowanie zgodności z przepisami i odpowiednią segmentację zasad. Dzięki temu można zmniejszyć ryzyko i ograniczać zagrożenia poprzez dynamiczną kontrolę dostępu do sieci, ocenę luk w zabezpieczeniach i wykorzystywanie informacji o zagrożeniach, a także poddawać kwarantannie podejrzane urządzenia.

Silnik Identity Services Błyskawiczne powstrzymywanie zagrożeń dzięki rozwiązaniom Cisco

„Rozwiązanie Cisco pozwala nam bardzo precyzyjnie określić, kto usiłuje uzyskać dostęp i do czego. Dzięki temu możemy odpowiednio kategoryzować każdego użytkownika i stosować zbiór zasad dopasowany do wymogów bezpieczeństwa informacji”.
Roman Scarabot-Mueller, dyrektor ds. infrastruktury, Mondi Group International

4

Zabezpiecz oddziały

Wykorzystaj inteligentną sieć WAN, aby chronić rozbudowaną sieć, zapewniając szyfrowanie, wgląd w informacje i łatwość zarządzania na takim samym poziomie jak w sieci kampusowej. Blokuj ataki, zapewnij bezpieczną łączność i chroń się przed zagrożeniami, korzystając z sieci VPN, zapory, segmentacji sieci i silnych technik szyfrowania oraz funkcji zabezpieczeń, aby zagwarantować oddziałom niezbędny poziom bezpieczeństwa.

Inteligentna sieć WAN

5

Bądź zawsze o krok do przodu

Zabezpiecz infrastrukturę, systemy internetowe i użytkowników mobilnych – skorzystaj z elastycznych możliwości licencjonowania oprogramowania, które oferuje ochronę sieci w czasie rzeczywistym, aktualne informacje o najnowszych zagrożeniach, spójność zasad w obrębie całej sieci, a także możliwości szybszego rozwiązywania problemów związanych z bezpieczeństwem. Miej pewność, że dzisiejsza inwestycja w oprogramowanie będzie przynosić korzyści przez długi czas dzięki elastyczności, łatwej dostępności do aktualizacji i nowych wersji.

Elastyczne możliwości licencjonowania oprogramowania Cisco ONE

„Średni czas wykrywania [nowych] zagrożeń (TTD) za pomocą rozwiązań Cisco skrócił się do około 13 godzin – to znacznie mniej niż obecna (i nieakceptowalna) średnia w branży, wynosząca od 100 do 200 dni”.
Raport półroczny Cisco na temat cyberbezpieczeństwa, 2016 r.

Wszystko jest dobrze, dopóki nie stanie się coś złego. Nie traktuj sieci jak towaru. Po co ryzykować? Niech zabezpieczenia będą integralnym elementem sieci. W ten sposób uzyskasz najwyższy poziom bezpieczeństwa – bez ograniczania sprawności działania – i zbudujesz bezpieczny fundament dla innowacji.

Już dziś rozpocznij podróż do cyfrowej architektury sieci.

Dowiedz się jak